HỌC PHẦN 7:

Phòng chống lạm dụng trực tuyến: Khi nhà báo và nguồn tin của họ bị tấn công

của Julie Posetti

Tóm tắt

Vấn đề tin xuyên tạc và tin sai[1] phá hoại báo chí uy tín và thông tin đáng tin cậy đã leo thang khủng khiếp trong thời đại truyền thông xã hội. Các hậu quả bao gồm việc tấn công một cách có chủ ý các nhà báo và các đơn vị xuất bản trực tuyến khác, cùng với các nguồn tin của họ, những người đang tìm cách kiểm chứng hay chia sẻ thông tin và bình luận. Những rủi ro liên quan có thể làm suy yếu hơn nữa lòng tin vào báo chí, cũng như sự an toàn của nhà báo và nguồn tin của họ.

Trong một số trường hợp, các nhà báo trở thành mục tiêu của những hành động "trồng cỏ giả"[2] và "chọc phá"[3] - những nỗ lực cố ý "đánh lạc hướng, đưa tin sai, lừa đảo, hay gây nguy hiểm cho các nhà báo"[4] với việc chia sẻ thông tin được thiết kế để làm rối trí và chỉ dẫn sai cho họ, hoặc các nguồn tin tiềm năng của họ. Ngoài ra, các nhà báo có thể trở thành mục tiêu bị lừa gạt để chia sẻ những thông tin không chính xác dẫn đến cách hiểu sai sự thật hoặc, khi điều đó bị lộ là giả, sẽ làm giảm uy tín của nhà báo (và tổ chức tin tức mà họ có mối liên kết). Trong các trường hợp khác, họ phải đối mặt với các mối đe dọa số được thiết kế để phơi bày nguồn tin của họ, xâm phạm quyền riêng tư để đẩy họ vào nguy hiểm hay xâm nhập vào thông tin chưa công bố của họ.

Ngoài ra còn xuất hiện hiện tượng các chính phủ huy động các "đội quân thù hận số" để giội gáo nước lạnh vào những bài bình luận phản biện và bóp chết tự do biểu đạt.[5] Sau đó là đến vấn đề nghiêm trọng của nạn quấy rối và bạo lực trực tuyến (đôi khi được gọi một cách mơ hồ là "chọc phá"[6]) đặc biệt giáng lên đầu phụ nữ và thường có bản chất thù ghét phụ nữ. Việc này có thể khiến các nhà báo, các nguồn tin của họ, và các nhà bình luận phải gánh chịu ầm ầm những lời lăng mạ trên mạng, những tuyên bố sai về tư cách của họ, sự xuyên tạc danh tính của họ, hay những lời đe dọa gây tổn hại được thiết kế để làm nhục họ và phá hoại sự tự tin của họ, làm giảm uy tín của họ, đánh lạc hướng họ và, cuối cùng là giội gáo nước lạnh vào công việc đưa tin của họ.[7] Trong khi đó ở nhiều nơi, nạn lạm dụng ở thế giới thật được thiết kế để bịt miệng báo chí phản biện vẫn tiếp tục,

1 Các định nghĩa có trong : Wardle, C. & Derakhshan, H. (2017). *Rối loạn thông tin: hướng tới một mô hình liên ngành cho nghiên cứu và hoạch định chính sách* (Hội đồng châu Âu). https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c [truy cập ngày 30/03/2018].

2 "Trồng cỏ giả" là một thuật ngữ bắt nguồn từ một thương hiệu có nhân tạo được sử dụng để trải thảm bề mặt ngoài trời để tạo ấn tượng như có tự nhiên. Trong bối cảnh tin xuyên tạc, nó liên quan đến việc lan truyền thông tin giả, tấn công khán giả và nhà báo với ý định chuyển hướng hoặc đánh lừa họ, đặc biệt dưới hình thức "bằng chứng" về sự ủng hộ giả dành cho một người, một ý tưởng hay một chính sách. Xem thêm định nghĩa của Technopedia: https://www.techopedia.com/definition/13920/astroturfing [truy cập ngày 20/03/2018].

3 Coco, G. (2012). *Tại sao không ai biết chọc phá là gì? Một hướng dẫn tham khảo nhanh cho truyền thông tại* Vice.com. https://www.vice.com/en_au/article/ppqk78/what-trolling-means-definition-UK-newspapers [truy cập ngày 30/03/2018].

4 Posetti, J. (2013). "*Twitter hóa" báo chí điều tra* trong S. Tanner & N. Richardson (Biên soạn), Nghiên cứu và điều tra báo chí trong một thế giới kỹ thuật số (trang. 88-100): Nhà xuất bản Đại học Oxford, Melbourne. http://ro.uow.edu.au/cgi/viewcontent.cgi?article=2765&context=lhapapers [truy cập ngày 30/03/2018].

5 Riley M, Etter, L and Pradhan, B (2018). *Một hướng dẫn toàn cầu về nạn chọc phá được nhà nước ủng hộ*, Bloomberg: https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/ [truy cập ngày 21/07/2018].

6 Ghi chú: "Troll", hay chọc phá, trong trường hợp liên quan đến mạng, chỉ các hành vi từ trêu chọc nhẹ nhàng, chơi khăm và khiêu khích cho đến lừa dối có chủ ý. Tuy nhiên, từ này càng ngày càng được dùng như một thuật ngữ để bao trùm tất cả các hành vi lạm dụng trực tuyến. Đây có thể là vấn đề vì nó đánh đồng một loạt các hoạt động và có khả năng xem nhẹ sự nghiêm trọng của nạn quấy rối trực tuyến.

7 Ví dụ, xem: https://www.independent.co.uk/news/world/americas/twitter-maggie-haberman-new-york-times-quits-social-media-jack-dorsey-a8459121.html

với nguy cơ ngày càng gia tăng vì được thổi bùng bởi những sự kích động và đe dọa trực tuyến.

Nhà báo có thể là nạn nhân trực tiếp của các chiến dịch tin xuyên tạc, nhưng họ cũng đang chống cự lại. Ngoài việc tăng cường phòng thủ kỹ thuật số, nhiều người còn chủ động phơi bày những cuộc tấn công này và vạch trần những kẻ tấn công. Tham gia vào các sáng kiến về Hiểu biết Truyền thông và Thông tin cùng với các tổ chức phi chính phủ trong không gian này, truyền thông tin tức cũng có vai trò trong việc giáo dục cho công chúng hiểu tại sao báo chí đáng được trân trọng và bảo vệ.

Đề cương

Bóc tách các vấn đề

i) Nhận diện và phản ứng với "chọc phá" và "trồng cỏ giả"[8]

Hiện tượng này bao gồm việc bịa ra các nhân vật và sự kiện để lừa gạt nhà báo và độc giả, cùng với các chiến dịch truyền thông xã hội có tổ chức có mục đích bắt chước phản ứng tự nhiên của công chúng. Chúng ta có thể khó phân biệt tin thời sự và những lời kể chính đáng của nhân chứng với nội dung đã bị làm giả hay bị thêm thắt những thông tin không chính xác để cố tình đánh lạc hướng hay làm giảm uy tín của các nhà báo và các nhà bình luận trực tuyến khác, cùng với công việc của họ, bằng cách lừa họ chia sẻ thông tin sai.

Ví dụ về loại hành vi này bao gồm:

- Bịa ra những nạn nhân thảm họa và những người thương vong trong các vụ tấn công khủng bố (xem ví dụ về vụ đánh bom ở Manchester[9]) để lừa mọi người chia sẻ nội dung có thể gây tổn hại đến danh tiếng và/hoặc uy tín của các cá nhân, bao gồm các nhà báo, những người có thể được gắn thẻ trong quá trình phân phối.

- Xuất bản một nội dung phô trương do các nhân vật hư cấu sản sinh ra như "Cô gái đồng tính ở Damascus"[10]. Vào năm 2011, truyền thông thế giới đã hò nhau để đưa tin về việc bắt giữ blogger tự cho là một người đồng tính nữ ở Syria này - tác giả hóa ra là một sinh viên Hoa Kỳ sống ở nước ngoài. Nhà báo Jess Hill đã được giao làm câu chuyện này cho chương trình PM của Đài Truyền hình Úc ABC. Cô nói rằng các giá trị và phương pháp kiểm chứng truyền thống đã ngăn chương trình của cô thổi phồng sự giả dối. "Chúng tôi đã không đưa tin về vụ bắt giữ cô ấy, vì một lý do đơn giản - chúng tôi không thể tìm thấy ai đã thật sự gặp mặt cô ấy. Không người thân, không bạn bè. Chúng tôi đã dành hai ngày để tìm kiếm, nhờ vả các mối liên hệ của chúng tôi ở Syria giới thiệu chúng tôi với những người có thể đã liên lạc với cô ấy,

8 Một giải thích hữu ích về "trồng cỏ giả" cho mục đích giảng dạy có thể tìm thấy trong đường dẫn có giá trị sau: https://youtu.be/Fmh4RdlwswE

9 Ví dụ về vụ đánh bom ở Manchester: https://www.theguardian.com/technology/2017/may/26/the-story-behind-the-fake-manchester-attack-victims [truy cập vào ngày 30/03/2018].

10 Young, K. (2017). *Làm sao để tự đánh lừa bản thân: trường hợp cô gái đồng tính ở Damascus*, ngày 09/11/2017, trên The New Yorker. https://www.newyorker.com/books/page-turner/how-to-hoax-yourself-gay-girl-in-damascus [truy cập vào ngày 30/03/2018].

nhưng mỗi đầu mối đều đi vào ngõ cụt. Việc chúng tôi không thể tìm thấy một ai đã thật sự gặp cô ấy đã gióng lên những hồi chuông báo động quan trọng, nên chúng tôi đã không đưa tin... Các cơ quan báo chí vội vàng đưa tin về câu chuyện đó đã không làm cái việc cơ bản là quay trở về với nguồn tin. Họ đã đưa tin dựa trên một bài viết blog."[11]

Những động lực khác là mong muốn chuyển hướng hay đánh lạc hướng nhà báo khỏi một cuộc điều tra bằng cách xúi giục hàng loạt hướng điều tra vô ích ngăn cản nỗ lực đưa tin và cuối cùng, có tác dụng làm tê liệt công tác tìm kiếm sự thật.

Những ví dụ về phong cách đánh lạc hướng này gồm có:

- Nỗ lực định nghĩa lại những tuyên bố về quy mô đám đông tại lễ nhậm chức của Donald Trump vào tháng 1/2017 như là "những sự thật khác'[12]
- Tuyên truyền chiến tranh đương đại, ví dụ: Taliban gửi tweet cho các nhà báo ở Afghanistan với các chi tiết sai và gây hiểu lầm về các trận đánh.[13]
- Các bộ dữ liệu được trao cho nhà báo cung cấp một số thông tin có thể kiểm chứng có giá trị cho lợi ích công nhưng đã bị hủy hoại vì có lẫn tin xuyên tạc trong đó.

Gần đây hơn, tuyên truyền điện toán[14] đã làm gia tăng rủi ro cho các nhà báo phải đối phó với hành động "trồng cỏ giả" và "chọc phá". Việc này liên quan đến việc sử dụng rô bốt mạng để phát tán thông tin sai và những thông điệp tuyên truyền có đích nhắm rõ ràng với quy mô được dàn dựng để tạo dáng vẻ một phong trào tự nhiên.[15] Đồng thời, công nghệ AI đang bị lợi dụng để tạo ra những video "giả sâu"[16] và các hình thức nội dung khác được thiết kế để làm mất uy tín các đối tượng mục tiêu, bao gồm các nhà báo, và đặc biệt là phóng viên nữ.

Ví dụ về những việc làm này bao gồm:

- Trang web tin tức độc lập Rappler.com và các nhân sự chủ yếu là nữ là mục tiêu trong của một chiến dịch lạm dụng trực tuyến quy mô. "Ở Philippines, những hành động chọc phá được trả tiền, lối suy luận ngụy biện, những cú nhảy cóc trong tư duy logic, lập luận kiểu đạp đổ - đây chỉ là một vài ví dụ

11 Posetti, J. (2013). Nguồn đã dẫn.

12 NBC News (2017). Video: https://www.nbcnews.com/meet-the-press/video/conway-press-secretary-gave-alternative-facts-860142147643 [truy cập vào ngày 30/03/2018].

13 Cunningham, E (2011). *Lúc thay ca, quân Taliban chơi truyền thông mới*, GlobalPost. https://www.pri.org/stories/2011-05-21/shift-taliban-embrace-new-media [truy cập vào ngày 30/03/2018].

14 Woolley, S. & Howard, P. (2017). *Tuyên truyền sử dụng điện toán trên toàn thế giới: tóm tắt chung*. Tài liệu nghiên cứu số 2017.11 (ĐH Oxford). http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf [truy cập vào ngày 30/03/2018].

15 Ghi chú: Những tin bài hời hợt về các chiến dịch rô bốt mạng trong cuộc tổng tuyển cử ở Anh vào năm 2017 nêu bật cái khó của việc đưa tin về những vấn đề này. So sánh với Dias, N. (2017). *Đưa tin trong một thời đại "trồng cỏ giả" kỹ thuật số mới*, First Draft News. https://firstdraftnews.com/digital-astroturfing/ [truy cập vào ngày 29/03/2018].

16 Thuật ngữ deepfake là một từ kết hợp "deep learning" (học tập chuyên sâu) và "fake" (giả mạo). Nó liên quan đến công nghệ AI dùng trong việc tạo ra nội dung gian trá, đôi khi có tính chất khiêu dâm, mà gần như không thể phát hiện được. Nó được sử dụng trong các cuộc tấn công mạng để làm mất uy tín của mọi người, bao gồm nhà báo. Xem: Cuthbertson, A (2018). *Khiêu dâm "giả sâu" là gì? Trí tuệ nhân tạo đưa việc trao đổi mặt lên một tầm đáng lo ngại* trên Newsweek. http://www.newsweek.com/what-deepfake-porn-ai-brings-face-swapping-disturbing-new-level-801328 [truy cập vào ngày 17/06/2018].

trong số các kỹ thuật tuyên truyền đã góp phần làm thay đổi dư luận về các vấn đề then chốt".[17] (xem thảo luận mở rộng dưới đây)

- Một gia đình giàu có bị buộc tội nắm giữ các doanh nghiệp nhà nước và các chính trị gia then chốt ở Nam Phi đã thuê công ty quan hệ công chúng của Anh, Bell Pottinger để bày ra một chiến dịch tuyên truyền công phu. Công ty này lan truyền các thông điệp của mình thông qua một đế chế tin xuyên tạc bao gồm các trang web, truyền thông và một đạo quân Twitter được trả tiền nhằm vào các nhà báo, doanh nhân và chính trị gia với những tin nhắn lăng mạ, thù địch và những hình ảnh được chỉnh sửa, với mục đích làm nhục và phản công để vô hiệu hóa những cuộc điều tra.[18] Biên tập viên nổi tiếng Ferial Haffajee đã trở thành mục tiêu của một chiến dịch quấy rối trực tuyến trong giai đoạn này, khi hình ảnh của cô bị xử lý để tạo ấn tượng sai về nhân cách cô, cùng với việc triển khai hashtag #presstitute[19] (phò báo chí).

- Trường hợp của nhà báo Rana Ayyub đã khiến năm báo cáo viên đặc biệt của Liên Hiệp Quốc phải gọi cho chính phủ Ấn Độ để yêu cầu bảo vệ cô, sau khi thông tin sai được lưu truyền tràn lan để phản kích tin bài phản biện của cô. Nhà báo độc lập này đã phải hứng chịu một sự kết hợp của tin xuyên tạc về cô trên truyền thông xã hội, bao gồm các video "giả sâu" vu khống cô từng làm phim khiêu dâm, cũng như những lời đe dọa hiếp giết trực tiếp[20]

- Trường hợp của nhà báo Phần Lan, Jessikka Aro, được thảo luận ở mục "Các mối đe dọa về an toàn kỹ thuật số và các chiến lược phòng thủ" trong phần ii) của học phần này.

Các học phần khác trong sổ tay này nói cụ thể về các kỹ thuật kiểm chứng chuyên môn, nhưng học viên cũng cần có khả năng nhận diện những động cơ hiểm ác của một kẻ vận hành trực tuyến trong việc sáng tác, phân phối và tấn công các nhà báo bằng tin xuyên tạc và tin sai như là một phần của mô hình lạm dụng.

Các câu hỏi quan trọng để bổ sung cho các phương pháp kỹ thuật kiểm chứng thông tin:

1. Có ý đồ hiểm ác nào ẩn đằng sau chia sẻ hay thẻ này không?
2. Người đăng nội dung này sẽ đạt được gì bằng việc chia sẻ?
3. Hậu quả đối với tôi/uy tín nghề nghiệp của tôi/một tổ chức truyền thông tin tức hoặc một nhà tuyển dụng là gì, nếu tôi chia sẻ nó?

17 Ressa, M. (2016). *Cuộc chiến tuyên truyền: vũ khí hóa mạng*, Rappler. https://www.rappler.com/nation/148007-propaganda-war-weaponizing-internet [truy cập vào ngày 30/03/2018].

18 Hồ sơ đầy đủ về "đế chế tin giả" của gia tộc Gupta có thể được xem tại: https://www.timeslive.co.za/news/south-africa/2017-09-04-the-guptas-bell-pottinger-and-the-fake-news-propaganda-machine/. [truy cập vào ngày 30/03/2018].

19 Haffajee, F. (2017). *Ferial Haffajee: nhà máy tin giả Gupta và tôi.* HuffPost South Africa. [bản trực tuyến]. Truy cập tại: https://www.huffingtonpost.co.za/2017/06/05/ferial-haffajee-the-gupta-fake-news-factory-and-me_a_22126282/ [truy cập vào ngày 06/04/2018].

20 *Các chuyên gia LHQ kêu gọi Ấn Độ bảo vệ nhà báo Rana Ayyub khỏi chiến dịch thù hận trực tuyến.* http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23126&LangID=E; [truy cập vào ngày 17/08/2018 See also Ayyub, R. (2018). Đọc thêm Ayyub, R. (2018). *Ở Ấn Độ, các nhà báo phải đối mặt với những lời lăng nhục và đe dọa hãm hiếp.* https://www.nytimes.com/2018/05/22/opinion/india-journalists-slut-shaming-rape.html [truy cập vào ngày 17/06/2018].

4. Tôi đã làm việc đủ chăm chỉ để xác định danh tính/mối liên kết/độ tin cậy/động lực của cá nhân này (ví dụ như có phải họ đang tìm cách gieo rắc tin xuyên tạc hoặc thu lợi từ việc bán nội dung có được bằng cách bất hợp pháp mà không có lý do gì liên quan đến lợi ích công) chưa?

5. Đây là một người hay một rô bốt mạng?[21]

6. Nếu bạn nhận được một "kết xuất dữ liệu" từ một người tự nhận là người thổi còi, bạn có nên độc lập kiểm chứng nội dung trước khi xuất bản đầy đủ bộ dữ liệu đó không? Liệu có khả năng nó được thêm thắt tin xuyên tạc và tin sai để cố tình gây hiểu lầm hoặc làm mất uy tín không?

ii) Các mối đe dọa an toàn kỹ thuật số và các chiến lược phòng thủ

Các nhà báo, nhà bảo vệ nhân quyền và người viết blog/nhà hoạt động truyền thông xã hội càng ngày càng dễ bị tấn công mạng, và dữ liệu hoặc nguồn tin của họ có thể bị các nhân vật hiểm ác xâm phạm thông qua các hành vi lừa đảo, tấn công bằng phần mềm độc hại, và giả mạo danh tính.[22]

Một ví dụ về việc làm này:
Nhà báo điều tra từng đoạt giải thưởng Jessikka Aro, người làm việc cho đài truyền hình công lập của Phần Lan YLE, đã trở thành mục tiêu của các chiến dịch "chọc phá" có tổ chức từ năm 2014. Cô đã trải qua những mối đe dọa an toàn kỹ thuật số bao gồm những hành động giả mạo và bòn rút thông tin[23], chọc phá tiết lộ thông tin liên hệ cá nhân và lan truyền tin xuyên tạc về cô, chất đầy các ứng dụng nhắn tin và hộp thư của cô bằng những tin nhắn giận dữ. "*Tôi nhận được một cuộc gọi mà nghe thấy tiếng người bắn súng ở trong đó. Sau đó, có người nhắn tin cho tôi, tự nhận là người cha đã mất của tôi và bảo rằng anh ta đang 'quan sát' tôi*".[24] Aro đã bày tỏ sự trân trọng đối với những biên tập viên biết bảo vệ phóng viên trước những lời đe dọa và thôi thúc các nhà báo điều tra và phơi bày tin tuyên truyền.

Do đó, điều quan trọng với những người hoạt động báo chí là phải cảnh giác trước các mối đe dọa sau:

12 mối đe dọa an ninh kỹ thuật số then chốt[25]

- Giám sát có mục tiêu và giám sát hàng loạt

21 Ví dụ, xem https://botcheck.me

22 Từ Technopedia: Spoofing hay lừa đảo là một việc làm gian trá hoặc hiểm ác mà trong đó thông tin giao tiếp được gửi từ một nguồn không xác định được ngụy trang là một nguồn mà người nhận quen biết. Email giả mạo là hình thức phổ biến nhất của việc làm này. Một email giả mạo cũng có thể chứa các mối đe dọa khác như Trojan hoặc các loại virus khác. Các chương trình này có thể gây thiệt hại đáng kể cho máy tính bằng cách kích hoạt các hoạt động không mong muốn, truy cập từ xa, xóa các tệp tin và hơn thế nữa: https://www.techopedia.com/definition/5398/spoofing [truy cập vào ngày 29/03/2018].

23 Từ Technopedia: Doxing hay bòn rút thông tin là quá trình truy xuất, tấn công an ninh mạng và công khai thông tin về người khác như tên, địa chỉ, số điện thoại và thông tin thẻ tín dụng. Doxing có thể được nhắm đến một người cụ thể hoặc một tổ chức. Doxing có nhiều lý do, nhưng một trong những lý do phổ biến nhất là để ép buộc. Doxing là một thuật ngữ tiếng lóng có nguồn gốc từ chữ ".doc" vì các tài liệu thường được lấy và chia sẻ. Các tin tặc đã phát triển các cách khác nhau để bòn rút thông tin, nhưng một trong những phương pháp phổ biến nhất là lấy email của nạn nhân, sau đó lấy mật khẩu để mở tài khoản của họ để lấy thêm thông tin cá nhân. https://www.techopedia.com/definition/29025/doxing [truy cập vào ngày 29/03/2018].

24 Aro, J. 2016. *Cuộc chiến không gian mạng: Tuyên truyền và chọc phá là những công cụ chiến tranh*. European View. Sage Journals, tháng 6/2016, Tập 15, Ấn bản 1. http://journals.sagepub.com/doi/full/10.1007/s12290-016-0395-5 [truy cập vào ngày 20/07/2018].

25 Posetti, J. (2015). Nghiên cứu mới: *Phòng chống các mối hiểm nguy đang gia tăng đe dọa an toàn kỹ thuật số của nhà báo* (WAN-IFRA). https://blog.wan-ifra.org/2015/03/27/new-study-combatting-the-rising-threats-to-journalists-digital-safety [truy cập vào ngày 30/03/2018].

- Khai thác phần mềm và phần cứng mà mục tiêu không hề biết
- Tấn công giả mạo[26]
- Tấn công tên miền giả
- Tấn công xen giữa (MitM)[27]
- Tấn công từ chối dịch vụ (DoS) và Từ chối dịch vụ phân tán (DDOS)[28]
- Tấn công thay đổi giao diện website
- Tài khoản người dùng bị xâm phạm
- Đe dọa, quấy rối và ép buộc các mạng trực tuyến phải lộ diện
- Các chiến dịch tin xuyên tạc và bôi nhọ
- Tước đoạt các sản phẩm báo chí
- Lưu trữ và khai thác dữ liệu

Về các chiến lược phòng thủ, xem: *Xây dựng an toàn kỹ thuật số cho báo chí.*[29]

Về những ẩn ý đối với việc tương tác với nhà báo, nhà sản xuất phương tiện truyền thông của các nguồn tin bí mật và những người thổi còi, xem: *Bảo vệ nguồn tin báo chí trong thời đại số.*[30]

Nhận biết và kiểm soát nạn quấy rối, bạo lực trực tuyến

"Tôi đã bị gọi là một con điếm bẩn thỉu, đồ Di-gan chết tiệt, con Do Thái, điếm Hồi giáo, ký sinh trùng Hy Lạp, kẻ di cư kinh tởm, kẻ tâm thần ngu ngốc, đồ dối trá xấu xí, kẻ thù hằn thiên kiến. Họ liên tục bảo tôi hãy cút về nhà rồi tự sát không thì họ sẽ bắn chết tôi, cắt lưỡi tôi, bẻ từng ngón tay tôi. Họ liên tục đe dọa sẽ hãm hiếp tập thể và tra tấn tình dục tôi."[31] Đây là những lời của nhà báo nổi tiếng người Thụy Điển Alexandra Pascalidou, người đã làm chứng vào năm 2016 trước một phiên họp của Ủy ban châu Âu tại Brussels về những gì cô đã trải qua trên mạng.

26 King, G (2014). *Những cuộc tấn công giả mạo sắc bén: Cần cảnh giác trên phương diện kỹ thuật số*, CPJ. https://cpj.org/blog/2014/11/spear-phishing-attacks-underscore-necessity-of-dig.php [truy cập vào ngày 29/03/2018].

27 Technopedia định nghĩa về Tấn công xen giữa (MITM) như sau: "Một hình thức nghe lén trong đó thông tin giao tiếp giữa hai người dùng bị theo dõi và thay đổi bởi một bên trái phép. Nói chung, kẻ tấn công chủ động nghe trộm bằng cách chặn đứng một sự trao đổi tin nhắn khóa công khai và truyền lại tin nhắn trong khi thay thế khóa công khai bằng khóa riêng của mình". https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm [truy cập vào ngày 29/03/2018].

28 Xem định nghĩa của Technopedia. https://www.techopedia.com/definition/24841/denial-of-service-attack-dos b. https://www.techopedia.com/definition/10261/distributed-denial-of-service-ddos [truy cập vào ngày 29/03/2018].

29 Henrichsen, J. et al. (2015). *Xây dựng an toàn kỹ thuật số cho báo chí* (UNESCO). Paris. http://unesdoc.unesco.org/images/0023/002323/232358e.pdf [truy cập vào ngày 30/03/2018].

30 Posetti, J. (2017). *Bảo vệ nguồn tin báo chí trong thời đại số* (UNESCO). Paris. http://unesdoc.unesco.org/images/0024/002480/248054E.pdf [truy cập vào ngày 30/03/2018].

31 Posetti, J. (2016). *Nhà báo người Thụy Điển, Alexandra Pascalidou, miêu tả các mối đe dọa trực tuyến về tra tấn tình dục và lạm dụng đồ họa* trên tờ The Sydney Morning Herald, 24/11/2016. http://www.smh.com.au/lifestyle/news-and-views/swedish-broadcaster-alexandra-pascalidou-describes-online-threats-of-sexual-torture-and-graphic-abuse-20161124-gswuwv.html [truy cập vào ngày 30/03/2018].

Sự sinh sôi nảy nở trên toàn cầu của loại lạm dụng trực tuyến nhắm vào các nhà báo và các nhà bình luận nữ này đã khiến LHQ (bao gồm UNESCO[32]) và các cơ quan khác nhận ra vấn đề, và kêu gọi hành động và giải pháp.

Tổ chức An ninh và Hợp tác Châu Âu (OSCE) đã tài trợ một nghiên cứu chứng minh tác động quốc tế của nạn lạm dụng trực tuyến các nhà báo nữ, những mục tiêu chính của hành động "chọc phá thù hận".[33]

Nghiên cứu đó tiếp bước một đề tài của tổ chức nghiên cứu Anh, Demos, một nghiên cứu đã kiểm tra hàng trăm ngàn tweet và nhận thấy báo chí là phạm trù duy nhất mà phụ nữ bị lạm dụng nhiều hơn nam giới, khi "các nhà báo nữ và những người dẫn chương trình tin tức truyền hình bị lăng mạ nhiều gấp ba lần[34] so với đồng nghiệp nam". Từ khóa của những kẻ lạm dụng là «đĩ», «hiếp dâm» và «điếm».

Một đặc điểm nổi bật của nạn lạm dụng nhà báo nữ trực tuyến là việc sử dụng các chiến thuật tin xuyên tạc - những lời nói dối được lan truyền về tính cách hoặc công việc của họ như một phương tiện phá hoại uy tín, nhục mạ họ, và tìm cách làm chặn đứng công việc bình luận và đưa tin công khai của họ.

Bên cạnh đó những đe dọa bạo lực, bao gồm cưỡng hiếp và giết người, và hiệu ứng "chồng chất" (các cuộc tấn công hàng loạt tự nhiên, được tổ chức, hay do rô bốt thực hiện nhằm vào một cá nhân trên mạng) làm tình hình trầm trọng hơn.

Bản chất mật thiết của các cuộc tấn công này, thường nhận được trên thiết bị cá nhân vào sáng sớm và đêm khuya, càng gây ra sợ hãi. "Có những ngày tôi thức dậy với những lời bạo lực và ngủ thiếp đi với cơn thịnh nộ phân biệt chủng tộc và giới tính vang vọng bên tai. Nó giống như một cuộc chiến tranh liên tục, cường độ thấp", Pascalidou nói.

Ở Philippines, Giám đốc điều hành và Tổng biên tập Rappler Maria Ressa[35], là một nghiên cứu tình huống về việc chống nạn quấy rối trực tuyến tràn lan trong bối cảnh một chiến dịch tin xuyên tạc quy mô lớn có liên kết với Nhà nước. Là một cựu phóng viên chiến trường của *CNN* nhưng cô cho hay, không có kinh nghiệm nào ngoài chiến trường chuẩn bị tinh thần cho cô khi đối diện với một chiến dịch quấy rối trực tuyến kỳ thị giới tính ồ ạt và hủy diệt nhắm vào cô từ năm 2016. "Tôi đã bị gọi là xấu xí, con chó, con rắn, bị đe dọa hiếp và giết," cô nói. Ressa đã không còn đếm nổi số lần cô nhận được những lời dọa giết. Ngoài ra, cô còn là chủ đề của các chiến dịch hashtag như #BắtgiữMariaRessa và #ĐưaCôTaĐếnThượngviện, được thiết kế để kích động các đám đông trực tuyến chuyển sang chế độ tấn công, làm mất uy tín của cả Ressa và Rappler và ngăn cản tin tức của họ. "Từ đó bắt đầu một vòng xoáy im lặng. Bất cứ ai phản biện hoặc đặt câu hỏi về các vụ giết người phi pháp đều bị tấn công, tấn công một cách tàn bạo. Phụ nữ phải chịu đựng nhiều nhất. Và chúng tôi nhận ra rằng hệ thống đó được thiết lập để bịt miệng những ý kiến bất đồng - được thiết kế để làm cho các nhà báo

32 Posetti, J. (2017). *Chiến đấu với nạn quấy rối trực tuyến lan tràn: Maria Ressa* trong L. Kilman (Biên soạn) , nguồn đã dẫn. Xem thêm: Nghị quyết 39 của Đại Hội đồng UNESCO thứ 39 ghi nhận "các mối đe dọa cụ thể mà nhà báo nữ phải đối mặt, bao gồm quấy rối tình dục và bạo lực, cả trực tuyến lẫn ngoại tuyến." http://unesdoc.unesco.org/images/0026/002608/260889e.pdf [truy cập vào ngày 29/03/2018].

33 OSCE (2016). *Chống lạm dụng trực tuyến đối nhà báo nữ.* http://www.osce.org/fom/220411?download=true [truy cập vào ngày 30/03/2018].

34 Bartlett, J. et al. (2014). *Sự thù ghét phụ nữ trên Twitter*, Demos. https://www.demos.co.uk/files/MISOGYNY_ON_TWITTER.pdf [truy cập vào ngày 30/03/2018].

35 Maria Ressa là Chủ tịch Ban Giám khảo của Giải thưởng Tự do Báo chí Thế giới UNESCO-Guillermo Cano: https://en.unesco.org/prizes/guillermo-cano/jury.

phải ngoan ngoãn vâng lời. Chúng tôi không được đặt những câu hỏi khó, và chắc chắn là chúng tôi không được phản biện."[36]

Chiến lược chống trả của Maria Ressa bao gồm:

- Nhận thức sự nghiêm trọng của vấn đề
- Nhận thức các tác động tâm lý và tạo điều kiện hỗ trợ tâm lý cho các nhân viên bị ảnh hưởng
- Sử dụng báo chí điều tra như một vũ khí trong cuộc chiến[37]
- Đề nghị những độc giả trung thành giúp đẩy lùi và ngăn chặn các cuộc tấn công
- Thắt chặt an ninh trực tuyến và ngoại tuyến để đối phó với nạn quấy rối
- Công khai kêu gọi các nền tảng (ví dụ: Facebook và Twitter) làm việc tích cực hơn để hạn chế và kiểm soát đầy đủ hành động quấy rối trực tuyến

Khi đối phó với mối đe dọa càng ngày càng gia tăng của nạn quấy rối trực tuyến, một điều quan trọng không kém là thừa nhận hành động quấy rối ngoại tuyến vẫn đang tiếp diễn đối với các nhà báo nữ trong bối cảnh các chiến dịch đưa tin xuyên tạc. Ví dụ, nhà báo điều tra người Úc, Wendy Carlisle đã bị lăng mạ, lôi kéo và chen lấn trong một cuộc biểu tình của những người phủ nhận đổi khí hậu ở Úc vào năm 2011 trong khi làm phim tài liệu cho Đài phát thanh ABC. Việc này đã khiến cô phải rời khỏi sự kiện để đảm bảo an toàn.[38]

Mục tiêu của học phần

Học phần này sẽ: thông tin cho học viên về những rủi ro của lạm dụng trực tuyến trong bối cảnh "rối loạn thông tin"; giúp học viên nhận ra các mối đe dọa; và cung cấp các công cụ phát triển kỹ năng để hỗ trợ cuộc chiến chống lạm dụng trực tuyến. Những mục tiêu này là:

- Nâng cao nhận thức của học viên về vấn đề các tác nhân hiểm ác nhắm vào các nhà báo, các nguồn tin, và các nhà truyền thông trực tuyến khác trong các chiến dịch đưa tin xuyên tạc/ tin sai;
- Cho phép học viên nhận diện tốt hơn các hành động "trồng cỏ giả", "chọc phá", các mối đe dọa an toàn kỹ thuật số, và lạm dụng trực tuyến;

36 Posetti, J. (2017). *Chống nạn quấy rối trực tuyến làn tràn: Maria Ressa* trong Kilman, L. (Biên soạn), Tấn công một người là tấn công tất cả (UNESCO). http://unesdoc.unesco.org/images/0025/002593/259399e.pdf [truy cập vào ngày 30/03/2018].

37 Đây cũng là một chiến thuật được Ferial Haffajee triển khai trong nghiên cứu tình huống "rò rỉ thông tin Gupta" đã được tham chiếu ở trên. Cô đã sử dụng các kỹ thuật báo chí điều tra và "thám tử" bảo mật kỹ thuật số để vạch trần một số vụ chọc phá nhằm vào mình với mục đích làm mất uy tín công việc đưa tin về vụ bê bối của cô. Xem: https://www.news24.com/SouthAfrica/News/fake-news-peddlers-can-be-traced-hawks-20170123 [truy cập vào ngày 16/06/2018].

38 Carlisle, W. (2011). *Chương trình biểu diễn lưu động Lord Monckton*, Tin vắn, ABC Radio National. http://www.abc.net.au/radionational/programs/backgroundbriefing/the-lord-monckton-roadshow/2923400 [truy cập vào ngày 30/03/2018].

▷ Trang bị cho học viên để sẵn sàng chiến đấu theo một cách nhạy cảm về giới với các hành động "trồng cỏ giả", chọc phá, các mối đe dọa an toàn kỹ thuật số, và lạm dụng trực tuyến.

Kết quả đầu ra

Đến cuối học phần này, học viên sẽ:

1. Hiểu biết sâu sắc hơn về tác động của lạm dụng trực tuyến đối với các nhà báo, nền báo chí, sự chia sẻ thông tin và tự do biểu đạt;
2. Nhận thức tốt hơn về vấn đề các tác nhân hiểm ác tấn công các nhà báo và các nhà truyền thông trực tuyến khác trong các chiến dịch đưa tin xuyên tạc/ tin sai;
3. Hiểu các mối đe dọa đặc biệt đối với an nguy của phụ nữ hoạt động báo chí trực tuyến;
4. Có thể nhận ra các tác nhân hiểm ác trên mạng dễ dàng hơn, cùng với các vụ "trồng cỏ giả", chọc phá, các mối đe dọa an toàn kỹ thuật số, và lạm dụng trực tuyến;
5. Được trang bị tốt hơn để chống lại các hành động "trồng cỏ giả", chọc phá, các mối đe dọa an toàn kỹ thuật số và lạm dụng trực tuyến theo một cách nhạy cảm về giới.

Hình thức học phần

Học phần này được thiết kế để dạy trực tiếp hoặc trực tuyến. Theo dự định, học phần sẽ được thực hiện theo hai phần: Lý thuyết và thực hành

Liên kết giáo án với kết quả đầu ra

A. Lý thuyết

Giáo án học phần	Số giờ	Kết quả đầu ra
Một bài giảng tương tác và hỏi đáp (90 phút), có thể được truyền tải theo cách truyền thống hoặc thông qua một nền tảng hội thảo trên mạng, với mục đích khuyến khích sự tham gia từ xa. Nội dung giảng dạy có thể lấy từ phần lý thuyết và các ví dụ nêu trên. Tuy nhiên, giảng viên cũng nên kết hợp các nghiên cứu tình huống có liên quan đến văn hóa/ địa phương khi dạy học phần này.	60 - 90 phút	1, 2, 3, 4, 5

B. Thực hành

Giáo án học phần	Số giờ	Kết quả đầu ra
Một cuộc thảo luận/hướng dẫn (90 phút) trong môi trường lớp học truyền thống, hoặc thông qua một nền tảng học trực tuyến như Moodle, các nhóm trên Facebook hoặc các dịch vụ khác cho phép sự tham gia trực tuyến từ xa. Cuộc thảo luận/hướng dẫn có thể áp dụng hình thức sau: • Chia buổi hướng dẫn thành các nhóm gồm 3-5 người học • Mỗi nhóm sẽ được cung cấp một ví dụ về nội dung hiểm ác (ví dụ: tìm kiếm trên blog và các kênh truyền thông xã hội các nội dung được tạo ra để tấn công Maria Ressa, Jessikka Aro và Alexandra Pascalidou, những trường hợp được thảo luận trong học phần này) liên quan đến một chiến dịch tin xuyên tạc/tin sai/chọc phá/trồng cỏ giả/ lạm dụng trực tuyến • Mỗi nhóm phải: hợp tác đánh giá tài liệu (tìm hiểu về cá nhân/nhóm đứng đằng sau tài liệu); xác định rủi ro và các mối đe dọa (tham khảo nghiên cứu có liên quan về các tác động có trong các bài đọc gợi ý); đề xuất một kế hoạch hành động để phản hồi tài liệu (điều này có thể bao gồm hồi âm có chiến lược, báo cáo người dùng đó cho nền tảng hoặc cảnh sát nếu thích hợp, giao làm một bài báo về vấn đề này); viết một bản tóm tắt 250 từ về kế hoạch hành động của họ (sử dụng Google Docs hoặc một công cụ chỉnh sửa hợp tác tương tự) và gửi cho giảng viên/ trợ giảng xem	90 - 120 phút	1, 2, 3, 4, 5

Cấu trúc thay thế

Để đi sâu hơn vào việc xử lý các vấn đề này, học phần có thể mở rộng để chia thành ba bài học riêng biệt (mỗi bài được chia thành hai phần, như được miêu tả ở trên):

- ▷ Nhận biết và phản ứng với "chọc phá" và "trồng cỏ giả"
- ▷ Các chiến lược lập mô hình đe dọa[39] và phòng ngự kỹ thuật số
- ▷ Nhận biết và kiểm soát nạn quấy rối, bạo lực trực tuyến liên quan đến giới tính

39 Stray, J. (2014). *An ninh cho nhà báo, Phần hai: Mô hình hiểm họa.* https://source.opennews.org/articles/security-journalists-part-two-threat-modeling/ [truy cập vào ngày 2/03/2018].

Bài tập gợi ý

Viết một bài báo dài 1.200 từ, hoặc làm một tin âm thanh năm phút, một tin video ba phút, hoặc một đồ họa tương tác chi tiết dựa trên cuộc phỏng vấn với một hay nhiều nhà báo về những kinh nghiệm bị lạm dụng trực tuyến của họ (ví dụ: trở thành mục tiêu của tin xuyên tạc và/hoặc đối diện với các mối đe dọa an ninh kỹ thuật số như là một phần của một chiến dịch tin xuyên tạc và/hoặc bị quấy rối hay bị tấn công bởi bạo lực trực tuyến). Học nên trích dẫn những nghiên cứu uy tín trong bài báo của mình và giải thích ẩn ý của những tác động của những hiện tượng này đối với báo chí/tự do biểu đạt và quyền được biết của công chúng.

Bài đọc

Aro, J. 2016. *Cuộc chiến không gian mạng: Tuyên truyền và troll là những công cụ chiến tranh*. European View. Sage Journals, Tháng 6/2016, Tập 15, Ấn bản 1. http://journals.sagepub.com/doi/full/10.1007/s12290-016-0395-5 [truy cập vào ngày 20/07/2018].

Haffajee, F. (2017). *Nhà máy tin giả Gupta và tôi trên The Huffington Post*. http://www.huffingtonpost.co.za/2017/06/05/ferial-haffajee-the-gupta-fake-news-factory-and-me_a_22126282/ [truy cập vào ngày 29/03/2018].

OSCE (2016). *Chống lạm dụng trực tuyến với nhà báo nữ*. http://www.osce.org/fom/220411?download=true [truy cập vào ngàyd 29/03/2018].

Posetti, J. (2017). *Chống nạn quấy rối trực tuyến lan tràn*: Maria Ressa trong L. Kilman (Biên tập), Tấn công một người là tấn công tất cả (UNESCO 2017). http://unesdoc.unesco.org/images/0025/002593/259399e.pdf [truy cập vào ngày 29/03/2018].

Posetti, J. (2016). *Nhà báo Thụy Điển, Alexandra Pascalidou, miêu tả các mối đe dọa trực tuyến về tra tấn tình dục và lạm dụng đồ họa* trên tờ The Sydney Morning Herald, 24/11/2016. http://www.smh.com.au/lifestyle/news-and-views/swedish-broadcaster-alexandra-pascalidou-describes-online-threats-of-sexual-torture-and-graphic-abuse-20161124-gswuwv.html [truy cập vào ngày 29/03/2018].

Nhà báo không biên giới (2018) *Quấy rối trực tuyến các nhà báo: cuộc tấn công của những kẻ chọc phá*. Nhà báo không biên giới: https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf [truy cập vào ngày 20/8/18].

Riley M, Etter, L and Pradhan, B (2018) *Một hướng dẫn toàn cầu về hành động chọc phá được nhà nước ủng hộ*, Bloomberg: https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/ [truy cập vào ngày 21/07/2018].

Stray, J. (2014). *An ninh cho nhà báo, Phần hai: Mô hình hiểm họa*. https://source.opennews.org/articles/security-journalists-part-two-threat-modeling/ [truy cập vào ngày 02/03/2018].